5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/622,596	07/18/2003	Pu Paul Zhang	AESN3013	4307

23488 7590 05/02/2007

GERALD B ROSENBERG
NEW TECH LAW
260 SHERIDAN AVENUE
SUITE 208
PALO ALTO, CA 94306-2009

EXAMINER	
SALL, EL HADJI MALICK	
ART UNIT	**PAPER NUMBER**
2157	

MAIL DATE	DELIVERY MODE
05/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/622,596	ZHANG ET AL.	
	Examiner	Art Unit	
	El Hadji M. Sall	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-82* is/are pending in the application.

4a) Of the above claim(s) *1-10 and 32-82* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the application filed on July 18, 2003. Claims 1-10 and 32-82 are withdrawn. Claims 10-31 are pending. Claims 10-31 represent secure cluster configuration data set transfer protocol.

2. ***Election/Restrictions***

Restriction is required under 35 U.S.C. 121 and 372.

This application contains the following inventions or groups of inventions, which are not so linked as to form a single general inventive concept under PCT Rule 13.1.

In accordance with 37 CFR 1.499, applicant is required, in response to this action, to elect a single invention to which the claims must be restricted.

Group I, claim(s) 1-9, drawn to computer network managing classified in class 709, subclass 223.

Group II, claim(s) 10-31, drawn to network computer configuring classified in class 709, subclass 220.

Group III, claim(s) 32-41, drawn to key management using master key (i.e., key-encrypting-key) classified in class 380, subclass 281.

Group IV, claim(s) 42-52, drawn to access control or authentication classified in class 726, subclass 2.

Group V, claim(s) 53-58, drawn to multicomputer synchronizing classified in class 709, subclass 2487.

Group VI, claim(s) 59-64, drawn to computer network monitoring classified in class 709, subclass 224.

Group VII, claim(s) 65-72, drawn to reconfiguration classified in class 713, subclass 100.

Group VIII, claim(s) 73-78, drawn to distributed data processing classified in class 709, subclass 201.

Group IX, claim(s) 62-63, drawn to client/server classified in class 709, subclass 203.

Inventions XII-I are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I has separate utility such as "routinely exchanging status messages between said plurality of servers wherein said status messages identify changes in the mutual configuration of said plurality of servers, wherein each said status message includes encrypted validation data and wherein said plurality of servers stores respective configuration data including respective sets of data identifying the servers known to the respective servers as constituting said plurality of servers..." as supposed to invention II which "receiving, by a computer system, a version message from said communications network; b) verifying said version message using verification encryption data securely held by said computer system...", and

invention III which comprising "a processor operative to execute control programs; and b) a service program operative, through execution by said processor as a control program, to generate responses to predetermined client requests", and so on. See MPEP § 806.05(d).

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

During a telephone conversation with Gerald B. Rosenberg, the attorney of record, a provisional election was made without traverse to prosecute the invention of group II, claims 10-31.

Applicant in replying to this Office action must make affirmation of this election. Claims -10 and 32-82 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

3. ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 10, 14, 15, 16, 17, 26, 27 and 28 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. "version message", "common version", "staging said updated configuration" and "stage for use" are not disclosed in the specification.

4. ***Claim Rejections - 35 USC § 102***

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. Claims 10-31 are rejected under 35 U.S.C. 102(e) as being unpatentable over Wang U.S. 7,107,246.

Wang teaches the invention as claimed including methods of exchanging secure messages (see abstract).

As to claims 10, 17 and 21, Wang teaches a method of securely distributing configuration data over a communications network to a plurality of computer systems, each computer system operating to evaluate configuration data, as stored in respective configuration data stores, in response to service requests to determine respective responses, said method comprising:

a) receiving, by a computer system, a version message from said communications network (column 3, lines 25-27; abstract);

b) verifying said version message using verification encryption data securely held by said computer system (column 3, lines 29-34);

c) determining, based on said version message, to retrieve updated configuration data from a configuration data source server identified relative to said a version number message (column 20, lines 34-42; column 8, lines 13-23); and

d) installing updated configuration data to the configuration data store of said computer system as retrieved from said configuration data source server, wherein said updated configuration data is retrieved as an encrypted data block and wherein said step of installing includes locating predetermined configuration data within said encrypted data block and decrypting said predetermined configuration data (column 8, lines 13-51).

As to claim 11, Wang teaches the method of claim 10 wherein said locating step determines the location of said predetermined configuration data using location encryption data securely held by said computer system (figure 4).

As to claim 12, Wang teaches the method of claim 11 wherein said verification encryption data and said location encryption data are related to a private encryption key securely held by said computer system (column 5, lines 19-25).

As to claim 13, Wang teaches the method of claim 12 wherein said verification encryption data and said location encryption data are related to respective private encryption keys securely held by said computer system (figure 4).

As to claim 14, Wang teaches the method of claim 10 wherein said plurality of computer systems use a common version of said configuration data, wherein said step of installing finally installs said updated configuration data for use by said computer system and wherein said method further comprises the steps of:

a) staging said updated configuration data pending completion of the installation of said updated configuration data (column 8, lines 56-51); and

b) waiting for said plurality of computer systems to signal use of a common version of said configuration data whereupon said step of installing completes the installation of said updated configuration data (column 8, lines 13-51).

As to claim 15, Wang teaches the method of claim 14 wherein said computer system receives version message from each of the other ones of said plurality of computer systems (column 3, lines 25-27; abstract), wherein said step of determining

determines the latest version of configuration data in use or staged for use by each of the other ones of said plurality of computer systems, and wherein said step of waiting waits for each of the other ones of said plurality of computer systems to signal use of a common latest version of said configuration data (column 8, lines 13-51).

As to claim 16, Wang teaches the method of claim 15 wherein said plurality of computer systems to signal use of a common latest version of said configuration data through respective version messages (column 7, lines 47-53).

As to claim 18, Wang teaches the method of claim 17 wherein the computer systems of said cluster respectively execute a common network service application, wherein execution of said common network service application is dependent on a respective installed configuration data set, and wherein said step of coordinating provides for the mutually corresponding installation of said modified configuration data set by said computer systems whereby execution of said common network service application is consistent across the cluster of computer systems (column 7, lines 39-53; column 1, 26-47).

As to claim 19, Wang teaches the method of claim 18 wherein said modified configuration data set includes individual configuration data sets identified with respective computer systems of the cluster, wherein said modified configuration data set includes a plurality of private encryption keys and wherein said step of preparing

provides for the encryption of said modified configuration data using said plurality of private encryption keys (column 8, lines 13-51; figure 4).

As to claim 20, Wang teaches the method of claim 19 wherein said individual data sets are encrypted relative to respective ones of said plurality of private encryption keys and wherein a predetermined computer system of said cluster must hove a respective one of said plurality of private encryption keys to decrypt a corresponding one of said individual data sets from said encrypted configuration data set (column 8, lines 13-23).

As to claim 22, Wang teaches the method of claim 21 wherein said revised configuration data set includes a plurality of respectively encrypted current configuration data sets and wherein said step of decrypting includes the steps of:

a) locating said current configuration data set, as encrypted uniquely for said first server computer system, from among said plurality of respectively encrypted configuration data sets (column 5, lines 19-25; figure 12A); and

b) discretely decrypting said current configuration data set from said revised configuration data set (column 8, lines 16-17).

As to claim 23, Wang teaches the method of claim 22 wherein said first server computer system has a unique private decryption key and wherein said step of locating depends on the identification, by said first server computer system, of a representation

of said unique private decryption key in said revised configuration data set, whereby location and decryption of said plurality of respectively encrypted current configuration data sets is locked to the respective server computer systems of said server cluster (column 5, lines 18-35; figure 12A).

As to claim 24, Wang teaches the method of claim 23 wherein said revised configuration data set includes representations of the unique private decryption keys of the respective server computer systems of said server cluster and wherein said step of locating includes:

a) matching a predetermined representation of said unique private decryption key of said first server computer system with a corresponding one of said representations of said revised configuration data set (column 7, lines 39-53); and

b) determining, based on the matched representation of said unique private decryption key of said first server computer system, the location of said current configuration data set, as encrypted, from among said plurality of respectively encrypted configuration data sets (column 8, lines 45-51).

As to claim 25, Wang teaches the method of claim 24 wherein said representations of the unique private decryption keys are secure digests of the unique private decryption keys of the respective server computer systems of said server cluster (column 18, lines 9-12).

As to claim 26, Wang teaches the method of claim 21 wherein said operative configuration data set includes a first version identifier and wherein said step of identifying includes:

a) receiving, by said first server computer system, version messages from the other server computer systems of said server cluster, wherein each version message includes a second version identifier and identifies a version message source server computer system (column 7, lines 39-53; column 1, 26-47); and

b) determining, with respect to a predetermined version message, whether said second version identifier, relative to said first version identifier, corresponds to said revised configuration data set (column 20, lines 34-42; column 8, lines 13-23).

As to claim 27, The method of claim 26 wherein said step of identifying further includes a step of validating said version messages with respect to said first server computer system (column 17, lines 33-37).

As to claim 28, Wang teaches the method of claim 27 wherein said first server computer system has a unique private decryption key and wherein said step of validating depends on the identification, by said first server computer system, of a representation of said unique private decryption key in said version messages such that version messages lacking said representation are discarded by said first computer server computer system (column 5, lines 18-35; figure 12A).

As to claim 29, Wang teaches the method of claim 28 wherein said version message includes representations of the unique private decryption keys of the respective server computer systems of said server cluster and wherein said step of validating includes matching said representation of said unique private decryption key of said first server computer system with a corresponding one of said representations of said revised configuration data set (column 7, lines 39-53; figure 12A).

As to claim 30, Wang teaches the method of claim 29 wherein said representations of the unique private decryption keys are secure digests of the unique private decryption keys of the respective server computer systems of said server cluster (column 18, lines 9-12).

AS to claim 31, Wang teaches the method of claim 30 wherein said revised configuration data set includes said representations of the unique private decryption keys and a plurality of respectively encrypted current configuration data sets, wherein said step of decrypting includes the steps of:

a) matching, by said first server computer system, of said predetermined representation of said unique private decryption key of said first server computer system in said revised configuration data set (column 7, lines 39-53);

b) determining, based on the matched representation of said unique private decryption key of said first server computer system, the location of said current configuration data set, as encrypted, from among said plurality of respectively encrypted

configuration data sets (column 8, lines 45-51); and

c) discretely decrypting said current configuration data set from said revised configuration data set, whereby the location and decryption of said plurality of respectively encrypted current configuration data sets is locked to the respective server computer systems of said server cluster (column 8, lines 16-51).

6. *Citation of Relevant Prior Art*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Prior art: 20050235345; 20020078382; 20050172336.

7. *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to El Hadji M Sall whose telephone number is 571-272-4010. The examiner can normally be reached on 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

El Hadji Sall
Patent Examiner
Art Unit: 2157

ARIO ETIENNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100